STATE OF NORTH CAROLINA

FORSYTH COUNTY

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION
FILE NO. 22-CVS-4687

FILED
2022 OCT 26 P 12:38
FORSYTH CO., C.S.C.
BY

C.C., Individually and on behalf of Similarly Situated Persons,

Plaintiffs,

vs.

META PLATFORMS, INC. F/K/A FACEBOOK, INC., and

NOVANT HEALTH, INC.

Defendants.

COMPLAINT

COMES NOW Plaintiff, C.C., individually and on behalf of similarly situated persons, and sets forth the following against Meta Platforms, Inc. (f/k/a "Facebook, Inc".) ("Meta"), and Novant Health, Inc. ("Novant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel, which included, among other things, consultation with experts in the field of data privacy.

SUMMARY OF ALLEGATIONS

1. This is a class action brought by Plaintiff, individually and on behalf of all citizens who are similarly situated (*i.e.*, the Class Members), seeking to redress Defendants' violations of their privacy rights. Plaintiff and the other Class Members are patients of Novant Health ("Novant") who entrusted their Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Novant Health. Novant entered into an advertising agreement with Meta wherein Meta would be given access to Novant's patient database. Defendants shared Plaintiffs' PHI and PII with persons who are not authorized to have said PHI and PII. Defendants betrayed Plaintiffs'

trust by failing to safeguard and protect their PHI and PII properly and publicly disclosing their PHI and PII without authorization in violation of State and Federal law.

2. Founded in 2004 as a social networking website for college students, Meta has evolved into one of the largest advertising companies in the country.[1] To date, Meta generates nearly 98% of its revenue through advertising bringing in a grand total of $114.93 billion.

3. To power its advertising business, Meta collects data in a variety of ways, one of which is through its "Meta Pixel."

4. Meta Pixel is a snippet of code embedded on a third-party website that tracks a user's activity as the user navigates through a website. Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information they input into the website.[2]

5. For instance, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added something to their cart, as well as what they purchased.

6. Meta Pixel takes each of these pieces of information it harvests and sends it to Meta with information, such as the user's IP address, name, email, or phone number. Meta stores this data on its server, and, in some instances, for years on end.[3]

7. Third-party websites that incorporate Meta Pixel benefit from the ability to analyze a user's experience and activity on its website to assess the website's functionality and traffic. The third-party website also gains information about its customers through the Meta Pixel that can be used

---

[1] John Gramlich, *10 facts about Americans and Facebook.* (June 1, 2021), https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

[2] Meta Business Help Center, *About Meta Pixel*, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited September 1, 2022)

[3] The Markup, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients* (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-antiabortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients

to target/retarget them with advertisements, as well as to measure the results of advertisement efforts.

8. The benefit of third-party use of Meta Pixel to Meta, however, is far more sinister. When Meta Pixel is incorporated, unbeknownst to users and without their consent, Meta gains the ability to gather surreptitiously every user interaction with the website ranging from what a user clicks on to the personal information entered on a website. Meta aggregates this data against all websites. [4]

9. Meta Pixel is wildly popular and embedded on millions of websites, including 30% of the top 80,000 most popular websites.

10. Meta Pixel is incorporated on websites that are used to store and convey sensitive medical information intended to stay private. For example, Meta Pixel is embedded on the websites of 33 of the top 100 hospitals in America and on password-protected patient portals of seven health systems, such as Defendant Novant Health.

11. This data, which is Protected Health Information, includes, without limitation, health conditions, mental health conditions, HIV status, diagnoses, medical procedures, test results, treatment status, treating physicians, medications, allergies, and general PII.

12. The PHI and PII is obtained and used by Meta, as well as other parties, in connection with targeted advertising.

13. C.C. and the Class Members had their PHI and PII, harvested by Meta through the Meta Pixel tool without their consent, and continued to have their privacy violated when their

[4] About Facebook Pixel | Meta Business Help Center, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited on September 1, 2022); and Unique Metrics | Meta Business Help Center (facebook.com), https://www.facebook.com/business/help/283579896000936 (last visited on September 1, 2022).

PHI and PII was used for profit by Defendants when they allowed pharmaceutical and other companies to send targeted advertising related to their medical conditions.

14. As a result of Meta's illegal information gathering, Plaintiffs received advertisements that were specifically tailored to their PHI and PII, including sensitive medical information.

15. These advertisements were tailored and directed to Plaintiff and the Class Members by Meta as part of Meta's advertising business on which Meta profits from providing third parties with access to persons most likely to be interested in their products or services, otherwise known as the target audience.[5]

16. Meta knows that the PHI and PII collected through its Pixel on Novant's websites includes highly sensitive medical information but, in reckless disregard for patient privacy continues to collect, use, and profit from this information.

17. Likewise, Novant knew that by embedding Meta Pixel – a Meta advertising tool – they were sharing and permitting Meta to collect and use Plaintiffs' PHI and PII and profiting from the share of this information.

18. Defendants' actions constitute an extreme invasion of Plaintiff and Class member's right to privacy and violate federal and state statutory and common law.

19. Plaintiffs have standing to bring this action because as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiffs have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or

[5] *Help your ads find the people who will love your business*. Facebook Advertising Targeting Options | Meta for Business, https://www.facebook.com/business/ads/adtargeting?content_id=7ko93HYgrMsIy4k (last visited September 1, 2022)

(ii) the additional damages set forth in detail below, which are incorporated herein by reference. Defendants' wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PHI and PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the other Class Members' PHI and PII and not yet used the information will do so at a later date or re-sell it.

20. Plaintiff and the Class members have also suffered and are entitled to damages for the lost benefit of their bargain with Defendants. Plaintiff and Class members paid Novant for its services including protecting their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff and the Class members should have received when they paid for their services, and the value of what they did receive, services without adequate privacy safeguards. Plaintiff and members of the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiff and the members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

21. Defendants have been unjustly enriched by the unauthorized use of Plaintiff's and the Class Members' PHI and PII.

22. Additionally, because of Defendants' conduct, Plaintiff and members of the Class have been harmed in that Defendant has breached its common law fiduciary duty of confidentiality owed to Plaintiff and members of the Class.

23. Accordingly, Plaintiff and the other Class Members seek redress against Defendants for breach of fiduciary duty, breach of implied contract, invasion of privacy by the public disclosure of private facts, common law negligence, negligence per se, negligent training and supervision, and breach of fiduciary duty of confidentiality.

24. Plaintiff, individually and on behalf of the other Class Members, seeks all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

25. The Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because both Plaintiff and Defendant are citizens of the State of North Carolina and Defendant is a business operating, and licensed under, the laws of the state of North Carolina.

26. Venue is proper in Forsyth County, North Carolina, pursuant to N.C.G.S. §1-82 because Novant maintains its principal office at 2085 Frontis Plaza Boulevard, Winston Salem, North Carolina 27103, which is within Forsyth County.

PARTIES

27. Plaintiff, C.C., is a citizen and resident of Rowan County, North Carolina.

28. Defendant Meta Platforms, Inc., f/k/a Facebook, Inc. is a Delaware corporation with its principal place of business located at 1601 Willow Road, Menlo Park, California 94025.

29. Defendant Novant Health, Inc., formally known as Presbyterian Health Services

Corp. is a corporation operating in and incorporated under the laws of the state of North Carolina with its principal place of business at 2085 Frontis Plaza Boulevard, Winston Salem, North Carolina 27103. Defendant Novant Health, Inc., can be served at 2626 Glenwood Ave, Suite 550, Raleigh, North Carolina 27608.

BACKGROUND FACTS

30. Certain allegations are made upon information and belief.

31. Defendant Novant Health is a health care provider pursuant to state and federal law, providing health care and medical services to the general public.

32. Defendant Meta is a business associate of Novant Health pursuant to state and federal law, and by association subject to the privacy rules and regulations of Novant Health and state and federal law.

33. The duty of patient privacy is an independent, non-delegable duty which attaches to any Business Associate, person or entity, to have access to PHI from a covered entity.

34. As a part of its business operations, Defendants collect and maintain PHI and PII of its patients and customers.

35. Plaintiffs were patients of Novant Health and therefore, pursuant to state and federal law were patients of Meta. As patients, Plaintiff and the Class Members provided their PHI and PII to Defendants.

36. The duty to maintain health care confidentiality and privacy pursuant to state and federal law is a non-delegable duty and independently attaches to any person or entity who services patients who provide PHI and PII as part of medical treatment with health care providers.

37. As such, Plaintiffs entered into an implied contract with Defendants for the adequate protection of their PHI and PII.

38. Defendants are required to maintain the strictest privacy and confidentiality of Plaintiff and the proposed Class Members' medical records and other PHI and PII.

39. Defendant Novant posts its privacy practices online, at https://www.novanthealth.org/home/digital-privacy-policy.aspx

40. On August 12, 2021, Defendants sent a letter to Plaintiff and members of the proposed Class to inform them of a data security incident that impacted their PHI.

41. According to the letter, "In May 2020, a tracking pixel was placed on [Novant's] website…" ("the Breach")

42. Upon information and belief, Novant gave Meta full and complete access to its patient database containing PHI and PII.

43. In June 2022, upon investigation, Novant determined that PHI may have been disclosed to Meta.

44. Novant purposefully started an advertising campaign with Meta to obtain information from Plaintiff and the Class Members in order to recruit more patients and increase profits.

45. For over two years, Defendants disclosed PHI and PII to the public which was unchecked.

46. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and the other Class Members' name, email address, date of birth, physicians, treatment, medical condition and diagnosis.

47. Had Defendants stated that they would not protect Plaintiff's and the Class Members' PHI and PII, Plaintiff and the Class Members would not have provided their PHI and PII to Defendants.

48. Upon information and belief, the Breach affected hundreds of thousands of Defendants' patients.

49. As a direct and/or proximate result of Defendants' failure to properly safeguard and protect the PHI and PII of their patients, Plaintiff's and the other Class Members' PHI and PII was stolen, compromised and wrongfully disseminated without authorization.

50. Defendant had a duty to its patients to protect them from wrongful disclosures.

51. The timing of the August 12, 2022 notice letter was beyond the time frame required by applicable laws.

52. Defendant Novant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Novant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

53. Defendant Novant is a covered entity pursuant to the Health Information Technology Act ("HITECH")[6]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

54. Defendant Meta is a is a Business Associate of the Covered Entity Novant pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Meta must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

55. Defendant Meta is a Business Associate of Covered Entity Novant pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

56. The HIPAA and HITECH do not provide a private cause of action but the rules, which are procedural in nature, work in conjunction with the already established laws of privacy

[6] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

in the State of North Carolina to provide the standard of procedure by which Defendants should operate in protecting PHI and PII.

57. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

58. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

59. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

60. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

61. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in

violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

62. Under HIPAA:

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.[7]

63. HIPAA and HITECH obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

64. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

65. HIPAA further obligated Defendants to ensure that their workforces complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and

[7] 45 C.F.R. § 160.103

appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

66. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[8] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[9]

67. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

[8] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[9] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[10]

68. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured Protected Health Information.

69. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider and/or business associate to have security measures in place and train its employees and staff so that all its staff and employees know their roles in facility security.

70. Defendants failed to provide proper notice to Plaintiff and the Class Members of the disclosure.

71. Defendants failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

72. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class Members' compromised PHI and PII.

73. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendants' wrongful actions and/or inaction and the resulting Breach have

[10] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud[11] and medical fraud.

74. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/ about-identity-theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

75. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

76. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give

[11] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

77. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[12] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to the identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[13]

78. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011. Of those experiencing fraud, 43% reported their credit card numbers were stolen, and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

79. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment,

---

[12] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[13] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology,* cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

80. Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the other Class Members' prior expressed written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

81. Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the other Class Members' PHI and PII to unauthorized persons.

82. Upon information and belief, Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

83. Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the other Class Members' PHI and PII to protect against

anticipated threats to the security or integrity of such information. Defendants' unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

84. The actual harm and adverse effects to Plaintiff and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants' wrongful actions and/or inaction and the resulting Breach requires Plaintiff and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiff and the other Class Members have suffered and will continue to suffer, such damages for the foreseeable future.

85. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiff and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of

$1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id.* at 6.

86. Other statistical analyses are in accord. The GAO found that identity thieves use PHI and PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

87. As a result of the disclosure, Plaintiff and the other Class Members have experienced an increase in spam and other intrusions on their privacy and/or an increase in attempts to infiltrate their financial and medical information.

88. Defendants' misuse of Plaintiff's and the other Class Members' PHI and PII and Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the other Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or

medical fraud pressed upon them by the Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach and (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not

CLASS ACTION ALLEGATIONS

89. Pursuant to N.C. Gen. Stat. §1A-1, Rule 23, Plaintiff brings this class action as a class action on behalf of himself and the following citizens who are similarly situated individuals:

All citizens of North Carolina who were patients of Defendant Novant Health since August 2015 and whose PHI and/or PII were disclosed by Defendant Novant Health and Defendant Meta to unauthorized third parties.

90. On information and belief, the putative Class is comprised of hundreds of thousands of individuals making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

91. The rights of Plaintiff and each other Class Member were violated in a virtually identical manner as a direct and/or proximate result of Defendants' willful, reckless and/or negligent actions and/or inaction and the resulting Breach.

92. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a. Whether Defendants willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the other Class Members' PHI and/or PII;

b. Whether Defendants were negligent in failing to properly safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

c. Whether Defendants owed a duty to Plaintiff and the other Class Members to exercise reasonable care in safeguarding and protecting their PHI and/or PII;

d. Whether Defendants breached its duty to exercise reasonable care in failing to safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

e. Whether Defendants were negligent in failing to safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

f. Whether, by publicly disclosing Plaintiff's and the other Class Members' PHI and/or PII without authorization, Defendants invaded their privacy; and

g. Whether Plaintiff and the other Class Members sustained damages as a result of Defendants' failure to safeguard and protect their PHI and/or PII.

93. Plaintiff and his counsel will fairly and adequately represent the interests of the other Class Members. Plaintiff has no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiff's lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

94. Plaintiff's claims are typical of the other Class Members' claims in that Plaintiff's claims and the other Class Members' claims all arise from Defendants' failure to properly safeguard and protect their PHI and PII.

95. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and the other Class Members' claims. Plaintiff and the other Class Members have been harmed as a result of Defendants' wrongful actions and/or inaction and the resulting Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct.

96. Class certification, therefore, is appropriate pursuant to N.C. Gen. Stat. §1A-1, Rule 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

97. Class certification also is appropriate pursuant to N.C. Gen. Stat. §1A-1, Rule 23 because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

98. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendants will retain the benefits of their wrongdoing despite its serious violations of the law.

FIRST CAUSE OF ACTION -
VIOLATIONS OF NORTH CAROLINA UNFAIR AND DECEPTIVE PRACTICES ACT
(Against Defendant Meta Only)

99. The preceding factual statements and allegations are incorporated herein by reference.

100. Pursuant to N.C. Gen. Stat. §75-1, Defendant Meta had a duty to refrain from engaging in unfair or deceptive practices affecting commerce. Commerce includes all business activities.

101. Had Plaintiff and the Class Members known that their PHI and PII would be disclosed they would not have provided it to Defendant Novant who in turn provided it to Defendant Meta.

102. By making promises of privacy that were not kept. Defendants engaged in unfair and deceptive practices affecting commerce.

103. Defendant Meta as a Business Associate of Defendant Novant had a duty to maintain the privacy of Plaintiff's and the Class Members' confidential information.

104. Defendant Meta breached its duty of confidentiality with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

105. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential PHI and PII, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

106. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach;

b. improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

c. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

d. the increased risk of identity theft; and,

e. emotional distress. At the very least, Plaintiff and Class Members are entitled to nominal damages.

107. Plaintiff and the other Class Members are entitled to have and recover attorneys' fees, compensatory and treble damages from the Defendants in an amount in excess of

$25,000 as a result of Defendants' unfair and deceptive trade practices.

SECOND CAUSE OF ACTION -
BREACH OF IMPLIED CONTRACT
(Against Defendant Novant Only)

108. The preceding factual statements and allegations are incorporated herein by reference.

109. Plaintiff and the other Class Members, as part of their agreement with Defendants, provided Defendants their PHI and PII.

110. In providing such PHI and PII, Plaintiff and the other Class Members entered into an implied contract with Defendant, whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class members' PHI and PII.

111. Under the implied contract, Defendant was obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

112. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

113. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Class' confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

114. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach;

b. improper disclosure of their PHI and PII;

c. loss of privacy;

d. out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

e. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

f. the increased risk of identity theft; and,

g. emotional distress.

115. Plaintiff and the other Class Members are entitled to recover damages in an amount in excess of $25,000.00.

THIRD CAUSE OF ACTION - NEGLIGENCE (Against Both Defendants)

116. The preceding factual statements and allegations are incorporated herein by reference.

117. Defendants owed, and continues to owe, a duty to Plaintiff and the other Class Members to safeguard and protect their PHI and PII.

118. Defendants breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PHI and PII.

119. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PHI and PII would result in an unauthorized third parties gaining access to such information for no lawful purpose.

120. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

121. Plaintiff's and the other Class members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach

b. improper disclosure of their PHI and PII;

c. loss of privacy;

d. out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

e. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

f. the increased risk of identity theft; and,

g. emotional distress. At the very least, Plaintiff and the other Class members are entitled to nominal damages.

122. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

123. Plaintiff and the other Class Members are entitled to recover damages in an amount in excess of $25,000.00.

FOURTH CAUSE OF ACTION -
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS
(Against Both Defendants)

124. The preceding factual statements and allegations are incorporated herein by reference.

125. Plaintiff's and the other Class Members' PHI and PII was (and continues to be) sensitive and personal private information.

126. By virtue of Defendants' failure to safeguard and protect Plaintiff's and the other Class Members' PHI and PII and the resulting Breach, Defendants wrongfully disseminated Plaintiff's and the other Class Members' PHI and PII to unauthorized persons.

127. Dissemination of Plaintiff's and the other Class Members' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is, and will continue to be offensive to Plaintiff, the other Class Members, and all reasonable people. The unlawful disclosure of the same violates public mores.

128. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

129. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach;

b. improper disclosure of their PHI and PII;

c. loss of privacy;

d. out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

e. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

f. the increased risk of identity theft; and,

g. emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

130. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

131. Plaintiff and the other Class Members are entitled to recover damages in an amount in excess of $25,000.00.

FIFTH CAUSE OF ACTION - BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY (Against Both Defendants)

132. The preceding factual statements and allegations are incorporated herein by reference.

133. At all times relevant hereto, Defendants owed, and owes, a fiduciary duty to Plaintiff and the proposed class pursuant to North Carolina common law, to keep Plaintiff's medical and other PHI and PII information confidential.

134. The fiduciary duty of privacy imposed by North Carolina law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

135. Defendants breached its fiduciary duty to Plaintiff by disclosing Plaintiff's and the other Class Members' PHI and PII to unauthorized third parties.

136. As a direct result of Defendants' breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's confidential medical information, Plaintiff and the proposed Class Members suffered damages.

137. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Class's confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

138. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach;

b. improper disclosure of their PHI and PII;

c. loss of privacy;

d. out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

e. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

f. the increased risk of identity theft; and,

g. emotional distress.

139. Plaintiff and the other Class Members are entitled to recover damages in an amount in excess of $25,000.00.

SIXTH CAUSE OF ACTION -
NEGLIGENT TRAINING AND SUPERVISION
(Against Both Defendants)

140. The preceding factual statements and allegations are incorporated herein by reference.

141. At all times relevant hereto, Defendants owed a duty to Plaintiff and the Class to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their patients and their parents.

142. Defendants breached its duty to Plaintiff and the members of the Class by allowing its employees and agents to give access to patient medical records to an unauthorized user.

143. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Class' confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

144. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach;

b. improper disclosure of their PHI and PII;

c. loss of privacy;

d. out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

e. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

f. the increased risk of identity theft; and,

g. emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

145. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

146. Plaintiff and the other Class Members are entitled to recover damages in an amount in excess of $25,000.00.

SEVENTH CAUSE OF ACTION - NEGLIGENCE *PER SE* (Against Both Defendants)

147. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein.

148. Plaintiff and Class Members were under the medical care of Defendant Novant.

149. Defendant Novant is a covered entity for purposes of HIPAA and HITECH.

150. Defendant Meta is a business associate for the purposes of HIPAA and HITECH.

151. Plaintiff and Class Members are members of the class HIPAA and HITECH were created to protect.

152. Plaintiff's and Class Members' private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

153. Defendants gave protected medical information to an unauthorized third party or unauthorized third parties without the written consent or authorization of Plaintiff or Class Members.

154. Defendants gave protected medical information to unauthorized third parties without Plaintiff's or Class Members' oral consent or written authorization.

155. The information disclosed to an unauthorized third party or unauthorized third parties included private health information about medical treatment.

156. Defendants' disclosure of the private health information of Plaintiff and Class Members without consent or authorization is a violation of HIPAA and HITECH and is negligence *per se*.

157. Alternatively, Defendants violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiff from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

158. As a direct result of Defendants' negligence, Plaintiff and Class Members suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, increased infiltrations into their privacy through spam and/or attempted identity theft, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

159. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to:

a. the untimely and/or inadequate notification of the Breach;

b. improper disclosure of their PHI and PII;

c. loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach;

d. the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud;

e. the increased risk of identity theft; and,

f. emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

160. As a direct result of Defendants' negligence, Plaintiff's and Class Members' risk of being future victims of identity theft relative to what would be the case in the absence of Defendants' wrongful acts has significantly increased.

161. As a direct result of Defendants' negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiff and Class Members of, and/or protect Plaintiff and Class Members from, being a victim of identity theft or other identity-related crimes.

162. Plaintiff, individually and on behalf of the Class, seek actual damages for all monies paid to Defendants in violation of the HIPAA and HITECH. In addition, Plaintiff seeks attorneys' fees.

163. Plaintiff and the other Class Members are entitled to recover damages in an amount in excess of $25,000.00.

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. Judgment against Defendants, jointly and severally, for an amount in excess $25,000.00 for nominal, actual, compensatory and treble damages.

2. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representatives and appointing Plaintiff's counsel as Lead Counsel for the Class;

3. Declaring that Defendants breached its implied contract with Plaintiff and Class Members;

4. Declaring that Defendants negligently disclosed Plaintiff's and the Class Members' PHI and PII;

5. Declaring that Defendants has invaded Plaintiff's and Class Members' privacy;

6. Declaring that Defendants breached its fiduciary duty to Plaintiff and the Class Members;

7. Declaring that Defendants breached its implied contract with Plaintiff and the Class Members;

8. Declaring that Defendants were negligent by negligently training and supervising its employees and agents;

9. Ordering Defendants to pay actual damages to Plaintiff and the Class Members;

10. Ordering Defendants to properly disseminate individualized notice of the Breach to all Class Members;

11. For an Order enjoining Defendants from continuing to engage in the unlawful business practices alleged herein;

12. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff;

13. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

14. Ordering such other and further relief as may be just and proper.

This the 29th day of September, 2022.

Janet Ward Black
NC State Bar No. 12869
Ward Black Law
208 West Wendover Avenue
Greensboro, North Carolina 27401
Phone: (336) 333-2244 Fax: (336) 379-9415
E-Mail: jwblack@wardblacklaw.com

Gabriel Snyder
NC State Bar No. 52406
Ward Black Law
208 W. Wendover Ave.
Greensboro, NC 27401
Phone: (336) 510-2152 Fax: (336) 510-2169
E-Mail: gsnyder@wardblacklaw.com

To be admitted *Pro Hac Vice*:
Maureen M. Brady KS #22460
Lucy McShane KS #22517
McSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com
ATTORNEYS FOR PLAINTIFFS